Office of the Information and
Privacy Commissioner of Alberta

PERSONAL INFORMATION PROTECTION ACT
Breach Notification Decision

Organization providing notice under section 34.1 of PIPA	Newegg Inc. (Organization)
Decision number (file number)	P2019-ND-039 (File #011034)
Date notice received by OIPC	December 4, 2018
Date Organization last provided information	December 4, 2018
Date of decision	February 28, 2019
Summary of decision	There is a real risk of significant harm to the individuals affected by this incident. The Organization is required to notify those individuals whose personal information was collected in Alberta, pursuant to section 37.1 of the *Personal Information Protection Act* (PIPA).
JURISDICTION	
Section 1(1)(i) of PIPA "organization"	The Organization is an "organization" as defined in section 1(1)(i) of PIPA.
Section 1(1)(k) of PIPA "personal information"	The incident involved all or some of the following information: • name, • address, and • payment card number, expiry date, and security code This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. The information was collected via the Organization's website. To the extent the personal information was collected in Alberta, PIPA applies in this matter.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	

Description of incident	• On September 18, 2018, the Organization became aware of a potential security incident involving unauthorized code on its website. • Based on its investigation, the Organization believes an unauthorized party gained access to its network using malicious software and then used that access to place unauthorized code on the Organization's website that handles customer transactions. • The unauthorized code was designed to capture customer order information as it was entered, bypassing other technical controls in place to protect order information. • On October 15, 2018, the investigation determined that the unauthorized code on the site may have collected the personal information at issue for orders placed on the website using a payment card, between August 13, 2018, and September 19, 2018.
Affected individuals	The incident affected 1,365 individuals.
Steps taken to reduce risk of harm to individuals	• Enhancing network and website security controls. • Implemented additional controls to automatically review the website's code and detect unauthorized changes. • Implemented additional access controls on the systems associated with the website to help prevent an unauthorized user from accessing and changing the website's code. • Notified the card brands of the incident.
Steps taken to notify individuals of the incident	A preliminary notification was emailed to affected individuals on September 19, 2018. A follow-up notification was emailed on November 16, 2018.
REAL RISK OF SIGNIFICANT HARM ANALYSIS	
Harm Some damage or detriment or injury that could be caused to affected individuals as a result of the incident. The harm must also be "significant." It must be important, meaningful, and with non-trivial consequences or effects.	The Organization reported "The possible harms that may occur as a result of the breach is the potential for fraudulent charges being made using the customer's payment card information." I agree with the Organization's assessment. In my view, a reasonable person would consider that the contact and financial information at issue could be used to cause the significant harms of identity theft and fraud.

Real Risk The likelihood that the significant harm will result must be more than mere speculation or conjecture. There must be a cause and effect relationship between the incident and the possible harm.	The Organization reported "The likelihood that harm will result is neutral" and described its efforts to notify affected individuals with a preliminary email sent September 19, 2018, and then a follow-up communication. The Organization also noted that "In many cases, payment card rules limit or eliminate liabilty [sic] for fraudulent charges that are timely reported by cardholders". In my view, a reasonable person would consider that the likelihood of harm resulting from this incident is increased because the personal information was compromised due to the malicious action of an unknown third party (deliberate intrusion and malware). The information was exposed for over a month. The Organization can only speculate that affected individuals may not be held responsible for any credit card fraud and misuse. Even if this were the case, it does not necessarily mitigate the potential harm from identity theft or other forms of fraud.

DECISION UNDER SECTION 37.1(1) OF PIPA

Based on the information provided by the Organization and given the circumstances of the incident, I have decided that there is a real risk of significant harm to the affected individuals.

A reasonable person would consider that the contact and financial information at issue could be used to cause the significant harms of identity theft and fraud. The likelihood of harm resulting from this incident is increased because the personal information was compromised due to the malicious action of an unknown third party (deliberate intrusion and malware). The information was exposed for over a month. The Organization can only speculate that affected individuals may not be held responsible for any credit card fraud and misuse. Even if this were the case, it does not necessarily mitigate the potential harm from identity theft or other forms of fraud.

I require the Organization to notify the affected individuals whose personal information was collected in Alberta in accordance with section 19.1 of the *Personal Information Protection Act Regulation* (Regulation).

I understand a preliminary notification was emailed to affected individuals on September 19, 2018. A follow-up notification was emailed on November 16, 2018. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner